社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－DPS－130 (63)
2007－CSEC－ 36 (63)
2007／3／2

非常時通報機能を有するオンライン手書き署名認証方式の提案

國井 雅* 遠藤 良輔* 有沢 大輔† 四方 順司*† 松本 勉*†
横浜国立大学大学院 環境情報学府／研究院*
横浜国立大学工学部電子情報工学科†
〒240-8501 横浜市保土ヶ谷区常盤台 79-7
{kunii, endo, arisawa, shikata, tsutomu}@mlab.jks.ynu.ac.jp

あらまし 情報通信技術の発達，携帯端末の小型軽量化により，携帯端末を持ち歩き，サービスを街頭など公の場所で利用する場面が増えてきた．それに伴い，あらたに想定すべき攻撃がいくつか考えられる．著者らは，不正者が，正規のユーザを脅して認証を強制することで認証をパスしようとするという攻撃について着目し，ユーザ認証における非常時通報の必要性を考え，非常時通報手段の評価の指針について検討してきた．本論文では，オンライン手書き署名認証への非常時通報機能付加を検討し，実験によりその有効性を検証した．

An online-handwritten-signature system with duress alarm function

Masashi KUNII* Ryosuke ENDO* Daisuke ARISAWA†
Junji SHIKATA*† Tsutomu MATSUMOTO*†
Graduate School of Environment and Information Sciences
Yokohama National University*
Division of Electrical and Computer Engineering
Yokohama National University†
79-7, Tokiwadai, Hodogaya, Yokohama, 240-8501 Japan

Abstract **We have discussed the attack of forcing a regular user to pass the user authentication by threat. Therefore, we have proposed user authentication system with duress alarm function and discussed the index of the evaluation of its systems. In this paper, we proposed new system that online-handwritten-signature system with duress alarm function, and we describe and evaluate effectiveness of our proposal.**

1. はじめに

正規のユーザのみ利用できるサービスや，正規のユーザのみ入ることのできる場所が存在した際に，その人間を識別するためにユーザ認証が用いられる．これまで考えられてきたユーザ認証は，認証を要求している者が本人か否かの判別は可能であるが，どんな状況で認証を要求しているかについてはわからない．そのため，不正者がユーザを脅迫し認証を強制していたとしても，サービス提供者はそのことに気づくことができない．この攻撃を本論文では脅迫攻撃と呼ぶこととする．脅迫攻撃は，不正者がユーザの生体情報を偽造せずなりすましを行えるため，生体認証を利用する場合においても，考慮すべき攻撃のひとつと考えられる．

ここで，もし不正者に気づかれずに通報を行うことができるならば，そのような脅迫による不正行為を防止することができる．そのための手段として，非常時通報(Duress Alarm)機能を認証に持たせるという方に用いる秘密情報を2種類用意し，片方を通常の認証に，もう片方を通報に用いることで，脅迫を行っている不正者には気づかれずに，脅迫されていることをサービス提供者に伝える機能である．

これまでに，非常時通報機能付加にあたってどのような方式が望ましいか考察が行われ，評価の指針について検討がなされている[1][2][3]．具体的な認証方式としては，知識を用いた対話型ユーザ認証の行列方式への非常時通報機能の付加[1][2]や，指静脈と指を用いる順番を利用した非常時通報機能を有するユーザ認証[3]が提案されている．これらの認証はいずれもチャレンジ・レスポンス方式を用いて非常時通報を行うものである．パスワードのような値の固定された鍵を入力する認証方式は，覗き見をした後ユーザを脅迫する攻撃者に対して，用意した2種類の鍵が判別されてしまうことから安全ではない．

本論文では，チャレンジ・レスポンス方式を用いない非常時通報として，生体認証の1つであるオンライン手書き署名認証における非常時通報機能付加を提案する．人間の行動的特徴を利用することで観測攻撃を行う攻撃者による判別を困難にできると考えられる．そこで，オンライン手書き署名認証に対する署名動作中の筆圧を変化させることで非常時通報を行う方式を提案し，製品化されているサイン認証ソ

フトを用いた実験を通して方式の有効性を検証した.

2. 非常時通報機能を有するユーザ認証

非常時通報は, 通常の認証に用いる正常時鍵と通報に用いる非常時鍵の 2 つを使い分けることで実現する. 非常時通報のモデルを図 1 に示す.

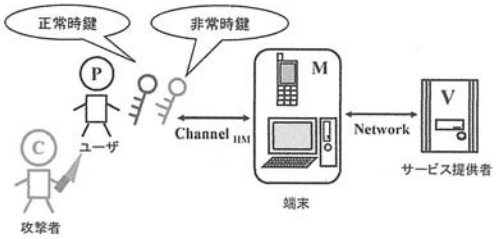

図 1 非常時通報のモデル

2.1 用語の定義

ここでは本論文で用いる用語の定義を行う.

認証行為:ユーザがあるサービス提供者に対して, サービス利用者であることを認証してもらう際の一連の流れ

正常時:脅迫されていない状況のこと

非常時:脅迫されている状況のこと

正常時鍵:ユーザが正常時の認証に用いる鍵

非常時鍵:ユーザが脅迫されていることをサービス提供者に通報したいときに用いる鍵

脅迫:ユーザを脅して秘密鍵を聞き出したり, 認証行為を強制したりすること

秘密鍵:認証に使用する鍵(正常時鍵と非常時鍵)の総称

応答:秘密鍵によって作成され, サービス提供者に対して提示する情報のこと

2.2 想定する環境

まず, 本論文で検討するユーザ認証を構成するエンティティを以下のように定義する.

ユーザ P:ある機関にその機関の提供するサービスの利用者として登録されている人間. 脅迫されている場合は, そのことを通報する人間

攻撃者 C: サービスの利用者を脅迫する人間

端末 M:認証に用いられる端末. ユーザとサービス提供者間の通信を媒介するデバイス

サービス提供者 V:認証を要求してきた利用者の状況を判定する悪意のないシステム. サービスを提供する機関によって安全に管理・運用されているもの

人間機械間通信路 $\mathbf{Channel_{HM}}$:サービス利用者と端末間の通信路. サービス利用者が提示情報を端末に提示する際に利用される

通信路 Network:サービス提供者と端末の間の安全な通信路

2.3 攻撃者の能力

Cの目的は, Pを脅して正常時の認証行為を行うよう強要する(強制)あるいはPになりかわって認証行為を行う(なりすまし)ことで, Vの認証を突破することである. C は$\mathrm{Channel_{HM}}$及び, P以外から情報を得ることはできない. また, このときPから得られる情報はPの意思によって決まるものとする. 具体的な攻撃手法は次の3種類の攻撃があり, これらの組み合わせによって攻撃が行われる.

認証過程の観測:脅迫に及ぶ以前の認証の認証過程を観測する攻撃. 観測にはビデオカメラなどの録画機器を利用する場合と, 目視による場合が考えられる

秘密鍵または応答の聞き出し:正常時, 非常時の両方の秘密鍵または応答を聞き出す攻撃. また, 鍵が複数ある場合はすべて聞き出す

認証行為の強制:ユーザに対して認証行為を強制する攻撃. 強制している間, ユーザが手に入れる情報は攻撃者も同じく手に入れることができる

2.4 非常時通報機能を有するユーザ認証に求められる要件

非常時通報機能を有するユーザ認証では, 非常時にユーザが鍵を入力する際, 攻撃者がユーザのすぐ隣に存在する, または, 攻撃者の監視下におかれる状況であっても, 攻撃者に気づかれることなく通報ができなければならない. またユーザ認証という側面を持ち合わせるため, 以下のように整理できる.

【要件 1】ユーザにとって正常時鍵と非常時鍵が使い分けやすいこと

具体的には,

- 秘密鍵が覚えやすく, 入力が簡易かつ再現性が高い
- 正常時の認証行為が非常時の認証行為を思い起こさせること

という項目がある.

【要件 2】攻撃者にとってなりすましが困難, かつ, 正常時鍵と非常時鍵の判別が困難であること.

安全性に関する要件は,

- なりすまし困難性
- 鍵の判別困難性

という 2 つを満たすことが求められる[3]. なりすまし困難性とは, ユーザ認証に求められる要件である. 鍵の判別困難性とは, 攻撃者に正常時鍵(または応答)と非常時鍵(または応答)が判別されない性質のことで, 非常時通報機能付加によって求められる要件である.

【要件 3】認証者は，正常時鍵と非常時鍵の判別を間違いなく行えること

具体的には，

- 認証精度が高い
- 認証エラーの割合が小さい
- 脅迫によってユーザが動揺をしても，正常時鍵または非常時鍵を安定して入力できる

という 3 つの項目を満たすことが求められる．

生体認証システムでは，誤拒否率，誤受理率という認証エラー割合を示す指標がシステムの評価に用いられる．本人の生体情報が本人のものでないと判断される割合を誤拒否率(FRR: False Rejection Rate)といい，異なる人間の生体情報で厳密には異なっているものが正しい本人の生体情報であると判断される割合を誤受理率(FAR: False Acceptance Rate)という．生体認証においては，あるユーザから本人か他人の生体情報が提示され，その情報が本人のものかそうではないかをシステムが判断するため，認証エラーは 2 パターンである．

一方，非常時通報機能を有するユーザ認証においては，提示された情報が，本人(正常時)・本人(非常時)・他人の 3 通りで，システムが下す判断は Accept(認証受理，以下 A)・Duress Alarm(非常時通報，以下 DA)・Reject(認証拒否，以下 R)の 3 通りとなる．正しく認証されるケースを除くと，認証エラーは以下の 6 通りになる．

i. 本人(正常時)が DA と判断される誤通報
ii. 本人(正常時)が R と判断される本人拒否
iii. 本人(非常時)が A と判断される誤受理
iv. 本人(非常時)が R と判断される通報拒否
v. 他人が A と判断される他人受入
vi. 他人が DA と判断される他人通報

生体認証への非常時通報機能付加を検討する場合はそれぞれの割合を評価の指標として取り入れる必要がある．

2.5 先行研究

これまでに提案されてきた各方式は，チャレンジ・レスポンス認証方式で 2 種類の知識を使い分ける[1][2]，指の順番を利用する[3]など，いずれもユーザが記憶する情報で，通常の認証と非常時の認証に用いる鍵を区別していた．

文献[1][2]で提案された具体的な認証方式では，攻撃者が過去の認証履歴を認証過程の観測によって得ていると，その履歴に 2 つの鍵を使用することでどちらの鍵が通常の認証に用いられているかの判別が容易に行われる，という安全性を損なう問題がある．

文献[3]では，文献[1][2]での問題は解決されたが，鍵を使用する順番に加え，前回の認証に用いた鍵が何番であったかを次回の認証まで記憶しておかなければならず，認証の利便性が低下している．本論文では，行動的特徴を用いた生体認証技術を利用することで，これらの問題点を改善することができると考えられる．

3. オンライン手書き署名認証方式を用いた非常時通報

3.1 オンライン手書き署名認証方式における非常時通報の優位性

オンライン手書き署名認証方式とは，書き残された筆跡形状の情報に加え，書き始めから書き終わりまでの署名中の動作情報をユーザ認証に利用する方式である．多くの個人的な特徴の時系列情報を利用していることから，偽筆によるなりすましに対する耐性があるといえる．

認証に用いられる時系列情報には，攻撃者が認証過程の観測をしただけでは正確に特徴を捉えにくい情報が含まれている．そこで，署名中の動作情報に変化を加え，正常時鍵と非常時鍵を使い分けることで，攻撃者の観測に耐え得る非常時通報機能を実現できると考えられる．

オンライン手書き署名認証方式に利用される特徴情報としては，筆跡形状・筆順・筆圧・筆記速度・ペンの傾き・空中でのペンの動きなどがある[4][5]．攻撃者による認証過程の覗き見を考慮すると，筆跡形状・筆順など変化を加えたことがわかりやすい特徴情報と筆圧・筆記速度・ペンの傾き・空中でのペンの動きなど正確に特徴を入手しづらい特徴情報に分けられる．4 章で行った実験でサイバーサイン社の認証ソフト[4]を用いるため，その認証ソフトが認証に用いる特徴情報，筆跡形状・筆順・筆圧・筆記速度のうち，筆圧に着目し，筆圧への変化を使い分けることで通報を行う非常時通報方式を提案する．

3.2 筆圧を用いた非常時通報機能を有するオンライン手書き署名方式の登録・照合

以下に非常時通報機能を有するオンライン手書き署名認証方式の鍵の設定と登録・照合について述べる．

鍵の設定

正常時鍵：自然な署名動作(以下，無変化署名)
非常時鍵：筆圧に変化をくわえた署名

登録・照合の流れ

図 2 に非常時通報機能を有するオンライン手書き署名認証の登録・照合の流れを示す．

まず，登録フェーズでは正常時認証用の署名データと非常時通報用の署名データが入力される．それぞれの署名データは筆記区間の検出，時間正規化の処理の後，テンプレートとなる．

照合フェーズにおいては，照合用署名データは

登録時と同様に筆記区間の検出，時間正規化の処理をされる．そして，この処理されたデータと登録フェーズにおいて作成されたテンプレートがDPマッチングにより比較・照合される．その結果，Accept，Duress Alarm，Rejectのいずれかを出力する．

比較・照合時に関しては，登録用の署名データと照合用の署名データの比較を行う方法が2通り考えられる．ここでは登録用正常時署名データをX，登録用非常時署名データをY，照合用署名データをZとする．

1. ZとXを比較し，その後ZとYの比較を行う．ZとXの類似度の方が高ければAcceptを出力する．ZとYの類似度の方が高ければDuress Alarmを出力する．どちらの類似度もある一定の閾値を超えない場合，Rejectを出力する．
2. まずZとXを比較することで正規ユーザであるかどうかの判定を行う．その後，ZとYを比較することで正常時か非常時かの判定を行う．最終的に，判定結果に応じてAccept，Duress Alarm，Rejectのいずれかを出力する．

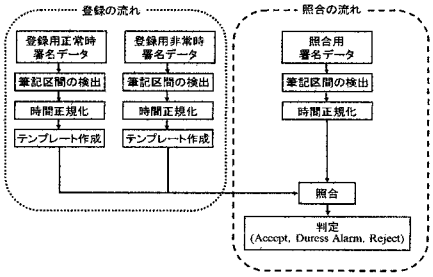

図2 非常時通報機能を有するオンライン手書き署名認証方式の登録・照合の流れ

3.3 想定する攻撃者の能力

オンライン手書き署名認証方式に非常時通報機能付加を検討する上で想定する攻撃者の能力については、以下のように設定する．

- CはPに対して脅迫攻撃，認証過程の観測(観測攻撃)が可能
- Cは認証に用いる装置の内部，および通信路を見ることはできない
- Cは認証に用いる装置の動作を改変できない
- Cは偽物の装置を使うことはできない
- Cは筆跡入力装置上に特殊な紙状のもの(カーボン紙等)を置くことはできない
- Cは，非常時通報用の署名が通常時の署名に何らかの変化を加えたものだということは知っている．ただし署名のどの部分の何に変化を加えているのかは知らない

4. 実験

第2.4節で整理した要件に関して，実験により提案方式の有効性を検証する．ユーザが加えた筆圧の変化がサイン認証アプリケーションにどのように判別されるのか(実験1)，筆圧への変化の加え方が第三者の観測攻撃にどの程度耐性があるのか(実験2)を知ることが実験の目的である．なお，本論文での実験では，1つの登録署名データと1つの照合用署名データを用いた照合が行われる認証ソフトを用いている．そのため，1の照合アルゴリズムに関する考察をすることができると考えられる．

実験を行う際に使用したタブレットの仕様を表1に示す．認証ソフトは，オンライン認証ソフト"C-SIGN LOCK for Tablet PC"を用いる．このソフトは，筆跡形状・筆順・筆圧・筆記速度・空中でのペンの動きを利用しての照合を行う．また，1(低)～10(高)のセキュリティレベルの設定と入力中の筆跡の表示・非表示の設定が可能である．

表1 タブレットの仕様

タブレット	Wacom社製"intuos3"PTZ-630
読取方式	電磁誘導方式
読取速度	最高200ポイント/sec
読取分解能	最高0.005mm
座標読取精度	±0.25mm
筆圧レベル	1024レベル
読取可能高さ	6mm(ペン)
傾き検出レベル	±60レベル

4.1 実験1

この実験では，サイン認証ソフトが無変化署名と筆圧へ変化を加えた署名をそれぞれが別の署名と判別できるかを検証した．また被験者を複数用意し，どのようなユーザでもサイン認証ソフトが判別できるような筆圧の変化を加えることができるかを検証した．

4.1.1 実験の概要

被験者を5名用意し，以下の手順で実験を行った．各Stepの試行回数は50回で，実験に使用する署名は被験者の名字を使用した．5名とも名字は漢字2文字で，そのうち1字の全画に筆圧に変化を加えた．加える変化は，無変化署名よりも筆圧を強く，無変化署名よりも弱く，の2パターンである．

サイン認証ソフトのセキュリティレベルは最も厳密に判断を行う10に設定し，入力中の署名は認証画面に表示する設定で実験を行った．

Step.1 「無変化署名」を登録し，そのテンプレート上で「無変化署名」を入力する．

Step.2 「無変化署名」を登録し，そのテンプレート上で「筆圧に変化を加えた署名」を入力する．

Step.3 「筆圧に変化を加えた署名」を登録し，そのテンプレート上で「無変化署名」を入力する．

Step.4 「筆圧に変化を加えた署名」を登録し，そのテンプレート上で「筆圧に変化を加えた署名」を入力する．

4.1.2 記号の定義

実験結果をまとめる際に用いた記号を以下のように定義する.

S_A :正常時用の署名(無変化署名)のこと
S_{DA}:非常時用の署名のこと
S_{PH}:筆圧を強くした非常時用の署名
S_{PL}:筆圧を弱くした非常時用の署名

4.1.3 各実験グループの検討

ユーザが登録した署名 S_{EN} と入力した署名 S_{IN} の組み合わせにより, 以下のようにグループ化する.

$(S_{EN} - S_{IN})$
$(S_A - S_A)$ → 通常時グループ
$(S_{DA} - S_{DA})$ → 非常時グループ
$(S_{DA} - S_A)$ → 誤通報グループ
$(S_A - S_{DA})$ → 誤受理グループ

実際に非常時通報機能を持ったオンライン手書き署名認証方式が存在することを想定した場合, 各グループの実験結果の意味は以下のようになる.

- 正常時グループ

S_A を入力したときに, S_A として受理されることを意味している. このグループの受理率が高いほど普段の認証行為をスムーズに行えるので, 利便性が高いといえる.

- 非常時グループ

S_{DA} を入力したときに, S_{DA} として受理されることを意味している. このグループの受理率が高いほど非常時用のサービスを正確に行うことができる.

- 誤通報グループ

S_A を入力したが, S_{DA} として受理されることを意味している. このグループの受理率が高いほど誤通報となりやすく, 非常時用のサービスが行われることになる. ユーザはそのたびにサービス提供者へ誤通報であることを説明し, 再度同じ内容のサービスを利用しなければならない. 誤通報が頻繁に発生する場合, サービスが成り立たなくなる.

- 誤受理グループ

S_{DA} を入力したが, S_A として受理されることを意味している. ユーザは通常時用の署名として受理されたことに気づけない. ユーザは通報したと判断しサービスを利用するため, 結果的に攻撃が成功する.

	S_A-S_A (正常時)	S_{PH}-S_{PH} (非常時)	S_A-S_{PH} (誤受理)	S_{PH}-S_A (誤通報)	S_{PL}-S_{PL} (非常時)	S_A-S_{PL} (誤受理)	S_{PL}-S_A (誤通報)
被験者1	100	100	32	100	100	16	100
被験者2	100	94	18	90	100	26	26
被験者3	100	98	2	6	100	76	98
被験者4	92	100	22	42	100	24	90
被験者5	98	96	6	0		6	

▨…テンプレート作れず　　単位 [%]

図 3 実験 1 の結果

4.1.4 結果

実験 1 の結果は図 3 に示す. 被験者 5 は, 無変化署名の筆圧が弱かったため, さらに弱くした署名では署名動作が認証ソフトには認識されず, テンプレートが作成できなかった.

4.2 実験 2

筆圧に変化を加える非常時通報方式が, 第 3 者の観測攻撃にどの程度耐性があるのか実験を行った. 実験1の被験者 3 の S_A の署名動作, S_{PH} の署名動作, S_{PL} の署名動作をビデオカメラでそれぞれ5回ずつ録画した. 録画した映像はすべて認証に成功した署名動作である. 録画した映像を用いて被験者に提示する映像を用意した. 被験者に提示する映像は, 画面を上下に二分したもので, 上下に流れる映像の組は, 以下の3パターンである. 実験の流れは以下の通りである.

① 上:S_A 下:S_A
② 上:S_A 下:S_{PH}
③ 上:S_A 下:S_{PL}

被験者に署名動作映像の組を 5 回提示する. 提示する映像の組は, 毎回①～③の中から無作為に選ぶ. 被験者は提示された映像組が①であるか, ②または③であるか, を判断する. 被験者は, ①である, ②または③である, わからない, の 3 つの選択肢の中から回答する.

実験1とは異なる被験者を 3 人用意し, 各署名のどの文字の筆圧を変化させているのかをあらかじめ伝えておいた. 被験者はその映像を何度も見直すことができるものとした. 実験の結果は, 被験者の回答がそれぞれ正解か, 不正解かを分けて図 4 に示す.

被験者の判断	①と判断		②or③と判断		わからない
	正解	不正解	正解	不正解	
被験者A	0	0	0	0	5
被験者B	0	2	2	1	0
被験者C	0	0	0	0	5

単位 [回]

図 4 実験 2 の結果

どの被験者も映像からでは2つの画面に表示される署名動作の組を明確に判別することは困難であるといえる.

5. 考察

5.1 実験1に関する考察

登録署名と入力した署名が同じものである場合, どの被験者も 100%に近い割合で受け入られていることがわかる. 被験者全員に共通することとして, 筆圧を変化させるに伴って, 筆圧以外の特徴情報も変化する傾向がある. これは誤受理グループと誤通報グループの受理率が低い要因の一つと考えられる. また, 実験 1 の結果から大きく分けて 2 つの傾向が

見て取れるため，その傾向について考察する．

まず，被験者3・被験者5の S_A- S_{PH}，S_{PH} - S_A の受理率が他の被験者に比べると極端に低かった．

この結果は，被験者3・被験者5の S_A 全体の筆圧が弱く，加えた筆圧の変化量が大きかったためと考えられる．また，被験者3の S_A - S_{PL}，S_{PL}- S_A の受理率が高くなったのは，S_A の筆圧がもともと弱く，認証ソフトが判別できるほどの差がつかなかったためと考えられる．一方，被験者 5 の S_A -S_{PL} の受理率は低くなった．これは被験者 5 の S_{PL} における筆跡形状がテンプレートを作成できないほど不安定であったため，筆跡形状の違いによるものであると考えられる．そこで，考察するにあたり，タブレットアプリケーション開発用Active-Xコントロール手書きコンポーネント評価版[6]を用いて，各被験者の筆圧データを採取した．採取するのは S_A の筆圧値で，そのデータから一画の平均筆圧を算出した．S_A 署名時の被験者 1,3,5 の一画の平均筆圧データは 1024 段階で 100～300 程度であり，その他の被験者に比べて低いことがわかった．S_A 全体の筆圧の弱い被験者 1 がこの傾向を示さなかったのは，筆圧の変化の加え方が弱かったためである．

次に，被験者 1,2,4 に関して，S_{PH}- S_A，S_{PL}- S_A では全体的に高い受理率となり．一方，S_A - S_{PH}，S_A - S_{PL} では約 20～30%の受理率であった．

この結果は S_{PH}，S_{PL} が普段行わない不慣れな署名であるから S_A に比べて S_{PH}，S_{PL} の入力は不安定になると考えられ，毎回の署名動作のばらつき具合が多くなる．このことより，S_{PH}，S_{PL} を登録署名として複数回入力しテンプレートを作成すると，テンプレートの作成時に設定される閾値が大きくなり，署名の受入範囲が広くなると考えられる．よって，入力署名 S_A がこの受入範囲に含まれやすくなり，S_{PH} - S_A，S_{PL}- S_A の受理率が高くなったと考えられる．一方，S_A は普段書き慣れている署名であることから，入力が安定している．よって，S_A を登録署名としたときのテンプレートは，S_{PH}，S_{PL} のものと比較すると受入範囲が狭くなると考えられる．入力署名 S_{PH}，S_{PL} が不安定であることから，このテンプレートの受入範囲にある程度含まれるので，約 20～30%の受理率となったと考えられる．

5.2 実験2に関する考察

実験 2 では，被験者は 3 人とも，2 つの映像が同じ署名動作か異なる署名動作か，映像からでは判別できなかった．しかし，実験 2 は音声のある映像を録画したため，筆記音を聞き分けることで，判別できる場合が多いことがわかった．また，漢字 2 字のうち 1 字全体の筆圧を変化させると変化を加える箇所が多く，観測攻撃によって判別されやすくなる．よって，変化を加える箇所を少なくすることで耐性を強くすることできると考えられる．

6. まとめと今後の課題

オンライン手書き認証方式への非常時通報機能付加を検討し，筆圧を用いた非常時通報機能を有するユーザ認証方式を提案した．実験1ではユーザが加えた筆圧の変化がサイン認証ソフトにどのように判別されるのか，実験2では筆圧への変化の加え方が第三者の観測攻撃にどの程度耐性があるのかを知るための実験を行った．

実験1より，筆圧に変化を加えた署名を非常時鍵とすることで，誤受理率が低くなること，誤通報率が高くなりやすいことがわかった．また，無変化署名の筆圧が強いユーザは筆圧の弱い署名を非常時鍵として，無変化署名の筆圧が弱いユーザは筆圧の強い署名を非常時鍵として設定することで，誤受理・誤通報の照合エラーを減らせると考えられる．実験2より，筆圧の強弱は映像から判別することは困難であることがわかった．しかし，筆記音などの認証に用いる特徴情報以外の情報から筆圧の強弱の判別がつきやすいことがわかった．

今後の課題としては，誤受理，誤通報などの認証エラーの割合を小さくするために，非常時通報に特化した照合アルゴリズムを実装し，照合精度の高い非常時通報機能を有するユーザ認証のアルゴリズムを検討する必要がある．また，筆記音などの認証に用いる特徴情報以外から署名動作が判別されることへの対策を考えることなどが挙げられる．さらに，脅迫という特異な状況下でユーザが通報を行おうと考えた場合，非常時鍵を正しく使用できるのか，という問題がある．行動的な特徴を用いた認証方式の場合，この要因はより大きく作用するため，今後検討すべき課題である．

参考文献

[1]大島康志，松本勉,“ユーザ認証における非常時通報,” 信学技報, Vol.103, No.315, pp.17-22, 2003.
[2]大島康志，松本勉,“ユーザ認証における非常時通報(その 2),” 信学技報，Vol.103, No.711, pp.145-150, 2004.
[3]古江岳大，遠藤良輔，四方順司，松本勉,“非常時通報機能を有するユーザ認証方式のモデル化,” 電子情報通信学会 2006 年暗号と情報セキュリティシンポジウム予稿集, pp.176, 2006.
[4]日本サイバーサイン社 HP
http://www.cybersign.com/index.html
[5]山中晋爾，浜本隆之，半谷清一郎，“署名時のペンの傾きによる筆者認証,” 電子情報通信学会 2000 年暗号と情報セキュリティシンポジウム予稿集, D6, 2000.
[6]株式会社ワコムアイティ,
http://www.wacom-it.co.jp/products/pen_conp/index.html (last visited 2006/01/28)